

MARKED-UP COPY

1. (Twice Amended) A method of securely providing data to a user's system over a web broadcast infrastructure with a plurality of channels, the method comprising the steps of:

- encrypting the data using a first encrypting key, wherein the first encrypting key is a symmetric key self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key;
- encrypting the first decrypting key, using a second encrypting key;
- broadcasting promotional metadata related to at least part of the encrypted data on a first web broadcast channel [fro] for reception by at least one user's system;
- broadcasting at least part of the encrypted data over a second broadcast channel; and
- transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key, to the user's system via a computer readable medium.

7. (Twice Amended) A method of securely receiving data on a user's system from a web broadcast infrastructure with a plurality of channels, the method comprising the steps of:

- receiving promotional metadata from a first web broadcast channel, the promotional metadata related to data available for reception;
- assembling at least part of the promotional metadata into a promotional offering for review by a user;
- selecting by a user, data to be received related to the promotional metadata;
- receiving data from a second web broadcast channel, the data selected from the promotional metadata, and wherein the data has been previously encrypted using a first encrypting key, wherein the first encrypting key is a symmetric key self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key]; and
- receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web broadcast channel.

19. (Twice Amended) A system for securely providing data to a user's system over a web broadcast infrastructure with a plurality of channels, the system comprising:

a content system;
a first public key;
a first private key, which corresponds to the first public key;
a data encrypting key[,];
a data decrypting key for decrypting data encrypted using the data encrypting key,
wherein the first encrypting key is a symmetric key [self-contained with all the information
necessary to decrypt the data encrypted with the first encrypting key];
first data encryption means for encrypting data so as to be decryptable only by the data
decrypting key;
second data encryption means, using the first public key, for encrypting the data
decrypting key;
a clearing house;
a broadcast center, for broadcasting to one or more user's systems on a first web
broadcast channel, promotional metadata related to data being broadcasted on a second web
broadcast channel, and broadcasting on the second broadcast channel data encrypted with the
data encrypting key;
first transferring means for transferring the data decrypting key which has been encrypted,
to the clearing house, wherein the clearinghouse possesses the first private key;
first decrypting means for decrypting the data decrypting key using the first private key;
a second public key;
a second private key, which corresponds to the second public key;
re-encryption means for re-encrypting the data decrypting key using the second public
key;
second transferring means for transferring the re-encrypted data decrypting key to the
user's system, wherein the user's system possesses the second private key; and
second decrypting means for decrypting the re-encrypted data decrypting key using the
second private key.

21. (Twice Amended) A user's system for securely receiving data from a web broadcast infrastructure with a plurality of channels, comprising:

a receiver for receiving promotional metadata from a first web broadcast channel, the promotional metadata related to data available for reception;

an interface to an output device for presenting at least part of the promotional metadata for review by a user;

an interface to an input device for receiving a selection by a user of the data to be received related to the promotional metadata;

a controller for controlling the receiver to receive data from a second web broadcast channel, the data selected from the promotional metadata, and wherein the data has been previously encrypted using a first encrypting key, wherein the first encrypting key is a symmetric key self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key]; and

an interface for receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web broadcast channel.

REMARKS

Applicants have studied the Office Action dated October 29, 2002 and have made amendments to the claims. It is submitted that the application, as amended, is in condition for allowance. By virtue of this amendment, claims 1-24 are currently pending in the present application. Reconsideration and allowance of the pending claims in view of the above amendments and the following remarks are respectfully requested. In the Office Action, the Examiner:

- (3-4) rejected claims 1, 7, 19, and 21 under 35 U.S.C. §112, second paragraph because the limitation "self-contained with all the information necessary to decrypt the data...";
- (5-6) rejected claims 1-3, 5, 7-16, and 21-24 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467);
- (7) rejected claims 4 and 6 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467) as applied to claim 1 above, and further in view of CableVision (periodical); and
- (8) rejected claims 17 and 18 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467) as applied to claim 7 above, and further in view of Horstmann (US 6,009,401).

The Applicants wish to thank Examiner Huseman for the telephone interview on January 15, 2003. Discussed was the meaning of the words "*self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key*" which the Applicants have been using to avoid the use of the negative term limitation "not a seed key." After the discussion, the Applicants have amended the claims to symmetric key as described in the specification. Inherent to a "symmetric key" is a self-contained key "*with all the information necessary to decrypt the data encrypted with the first encrypting key*" and which distinguishes a "seed key" as described in the Dillon references as further discussed below.

Final Office Action Is Inappropriate

Applicants have studied the Office Action dated October 29, 2002. Applicants respectfully request entry of these remarks under the provisions of 37 C.F.R. § 1.116(a) in that the remarks below place

the application and claims in condition for allowance, which allowance is respectfully requested. Reconsideration and allowance of the claims in view of the following remarks are respectfully requested.

As an initial matter, the Examiner made the Office Action Final. Applicants respectfully traverse this decision. In the Final Office Action, the Examiner ignored the claim language of "encrypting the first decrypting key using a second decrypting key" as recited in independent claims 1, 19, and 21. The Examiner on page 2 of her office action states: "Applicants have amended the above claimsAlso, how can the encrypting key be self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key when the encrypted first decrypting key, presumably used to decrypt the data encrypted with the first encrypting key, is transferred with a second encrypting key via a computer readable medium." (Emphasis in the original). As an initial point, the independent claims have been amended to include the limitation "all the information necessary to decrypt the data encrypted with the first encrypting key" to clearly distinguish over the "key seed ID" identifying the key seed needed to decrypt the document in Dillon '911 taken alone or in view of Dillon '467. Note the Applicants could use a negative claim limitation such as a first encrypting key not based on a seed key but chose a positive limitation for clarity to distinguish Dillon.¹ The Examiner at page 2 of her response is, respectfully, confounding the claim limitation of "encrypting the first decrypting key using a second decrypting key" with delivering two keys to the user's system. Unlike independent claims 1 and 19, independent claims 7 and 21 nowhere mention a second key. Rather independent claims 7 and 21 have been amended to distinguish over "key seed ID" of Dillon by reciting "wherein the first encrypting key is self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key." To clarify this limitation, the Applicants amended to recite "symmetric key." The term "symmetric key" is used as known in the specification as originally filed at pages 26 and 27. The term "symmetric key" is self-contained with all the information necessary to decrypt the data. Although the term "symmetric key" has been used as known in the art as "self-contained with all the information necessary to decrypt the data" it was not

¹ See §2173.05(i) Negative limitations in claims is not wrong so long as the boundaries of the patent protection sought are set forth definitely as they are here in the present invention.

ipsis verbis (not in the identical words) in the specification. The Examiner is respectively reminded that this was sufficiently described in the specification on pages 26-27, FIG. 6 and pages 42-45 as originally filed albeit not in the identical words.²

Continuing further, in independent claims 1 and 19 there are not two keys being transferred as the Examiner suggests, but rather only one key where the key has been encrypted with a second key. Turning to the claim language:

Claim 1

encrypting the data using a first encrypting key, wherein the first encrypting key is
a symmetric key;
transferring the encrypted first decrypting key, which has been encrypted with
the second encrypting key, to the user's system via a computer readable medium.

Claim 19

second data encryption means, using the first public key, for encrypting the
data decrypting key;
first transferring means for transferring the data decrypting key which has been
encrypted, to the clearing house, wherein the clearinghouse possesses the first private key;

According to MPEP § 706.07(a): "Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection not necessitated by amendment of the application by applicant, whether or not the prior art is already of record." In the previous Office Action dated May 16, 2002, the Examiner rejected claims 1-3, 5,

² "If, on the other hand, the specification contains a description of the claimed invention, albeit not in *ipsis verbis* (in the identical words), then the examiner or Board, in order to meet the burden of proof, must provide reasons why one of ordinary skill in the art would not consider the description sufficient. See *In re Alton* (Fed. Cir. 1996) (Emphasis Added). See also *Fujikawa v. Wattanasin* (Fed. Cir. 1996), *ipsis verbis*, "as the Board recognized, however, *ipsis verbis* disclosure is not necessary to satisfy the written description requirement of section 112. Instead, the disclosure need only reasonably convey to persons skilled in the art that the inventor had possession of the subject matter in question. *In re Edwards*, 568 F.2d 1349, 1351-52, 196 USPQ 465, 467 (CCPA 1978).

7-16, and 21-24 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (US 6,337,911) in view of Dillon (US 6,351,467). In the previously-filed amendment, Applicants amended the independent claims 1, 7, 18, and 21 for clarity and to include an additional limitation of “self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key.” The Examiner, respectfully, as shown above, clearly misinterpreted this limitation of an encrypting key not based on a “key seed.” The Applicants did not switch from one subject matter to another or resort to any subterfuge to keep the application pending.³ Thus, it is respectfully submitted that the final status of the Office Action is premature and should be withdrawn.

If the Examiner does not withdraw the final status of the Office Action, Applicants submit that this response does not raise new issues in the application. It is submitted that the present response places the application in condition for allowance or, at least, presents the application in better form for appeal. Entry of the present response is therefore respectfully requested.

Rejection Under 35 U.S.C. § 103(a) applying Dillon (6,337,911) in view of Dillon (6,351,467)
As noted above, the Examiner rejected claims 1-3, 5, 7-16, and 21-24 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467). As discussed in the Applicants’ response filed on August 29, 2002 and in the telephonic interview on January 15, 2003, the Dillon ‘911 reference teaches that the “key seed ID” is sent as opposed to a decrypting key as recited in the present invention. In the words of Dillon at col. 6, lines 57-58:

“After broadcast center 150 sends the announcement message for a document, it prepares to send the document itself. The document is packetized, encrypted, and broadcast over communications link 140. As broadcast receiver 120 receives each encrypted packet, it determines whether it is a packet for which broadcast receiver 120 has a key.” (Emphasis Added).

And, as the Examiner points out in Dillon at col. 6, lines 44-48:

³ See MPEP § 706.07.

"The announcement message is received and decrypted by broadcast receiver 120 and passed to file broadcast receiver 112. If the announced document is on the list of documents of interest, file broadcast receiver 112 sends a load request including the key seed ID to security engine 130." (Emphasis Added).

Accordingly, Dillon '911 teaches taking the "key seed ID" and encrypting it. The "key seed ID" as taught by Dillon is used to generate the decrypting key in security engine 130. See col. 4, lines 59-67 continuing onto col. 5, lines 1-6. In the words of Dillon at col. 8, lines 33-44:

"In executing function F3, broadcast center 150 periodically, e.g., monthly, sends account status information to each of the plurality of receiving computers, including receiving computer 110. The account information is tailored to the receiving computer and includes a statement of its receiver's status (e.g., satisfactory, overdrawn, limited access, etc.). The account information also includes core information required by security engine 130 to create keys to decrypt electronic documents. Although the account information is broadcast in the clear, the contents of the account information is encrypted in such a way that only security engine 130 may access and decrypt the account information." (Emphasis Added).

In contrast, the independent claims 1, 7, 19, and 21 of the present invention have been amended to describe the first encrypting key as "symmetric key." Support for this language is found in the present invention as originally filed in FIG. 6 items 623 and in the specification at least pages 43 - 150. This is very important since the self-contained key itself and not a "key seed ID" as taught by either of the Dillon references. The Dillon references nowhere teach or suggest such levels of security. In contrast Dillon is relying on pre-sending key information to the security engine 130 on a periodic basis so that the security engine 130 is able "to create keys to decrypt electronic documents." The present invention eliminates this step of pre-sending account status information on a periodical basis because in the present invention, the first encrypting key is "symmetric key." Dillon '911 teaches a symmetric encryption structure for at col. 5, line 23-36 (Emphasis Added):

Memory 304 includes a software program that is executed by CPU 302 to perform functions F10, F11, and F12 described in connection with the table below. A

preferred embodiment of the present invention uses software based encryption because the amount of data to be encrypted and decrypted by the security engine is relatively small and relatively slow encryption and decryption is acceptable. In contrast, broadcast receiver 120 preferably implements a decryption algorithm in hardware using a symmetrical encoding scheme, such as the Data Encryption Standard (DES) Electronic Codebook implemented under Federal Standard 10-26, as shown in Telecommunications: Compatibility Requirements for Use of Data Encryption Standards, published Dec. 11, 1978 by the General Services Administration.

However, this symmetrical encoding scheme as described by Dillon '911 is explicitly not used for the content itself but only for the account information including key seed for generating keys to decode the documents." See Dillon at 38-51. In contrast the symmetric key in the present invention is the key used to encrypt the data itself and not for holding key seeds to generated keys to decrypt the data as described by Dillon '911.

Accordingly, the present invention distinguishes over Dillon '911 taken alone or in view of Dillon '467 for at least this reason.

Continuing further for independent claims 1 and 19, no where does Dillon '911 taken alone or in view of Dillon '467 teach or suggest the higher level of security of re-encrypting the content decrypting key with a second key:

Claim 1

encrypting the first decrypting key, using a second encrypting key;

Claim 19

second data encryption means, using the first public key, for encrypting the data decrypting key;

This level of security which personalizes the decrypting key to each end-user device or system is nowhere suggested or taught by Dillon '911 taken alone or in view of Dillon '467 and the present invention distinguishes by Dillon '911 taken alone or in view of Dillon '467 for at least this reason

as well.

Continuing further, the present invention recites a second encrypting key which is a public key of a trusted third party i.e., Clearing house(s) 105. Dillon '911 taken alone or in view of Dillon '467 does not show this level of security control using public keys of trusted third parties rather Dillon is using a "key seed ID" which is sent to decrypt the document which has been decrypted. See at least Dillon '911 at col. 6, lines 57-58 and col. 6, lines 44-48. By using public key infrastructure, the present invention is not limited to pre-sending "key seed Ids" to generate local decryption keys at the security engine 130. The public key infrastructure allows any type of key to be used including keys of different lengths and therefore different encryption strengths. In the present invention each piece of content or data can be dynamically encrypted with a different type of key strength without the requirement to pre-send the decrypting key to an end user system as taught by Dillon '911. Accordingly, the present invention distinguishes over Dillon '911 taken alone or in view of Dillon '467 for at least this reason as well.

Moreover, the Federal Circuit has consistently held that when a §103 rejection is based upon a modification of a reference that destroys the intent, purpose or function of the invention disclosed in the reference, such a proposed modification is not proper and the *prima facie* case of obviousness can not be properly made. See *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Here the intent, purpose and function of Dillon 911 taken alone or in view of Dillon '467 is the use of "key seed Ids", in contrast the intent and purpose of the present invention is "*symmetric keys*." Not only does the present invention eliminate the need to "to create keys to decrypt electronic documents" in security engine 130 as required by Dillon, but the present invention makes use of the many advantages of a public key infrastructure. This combination, as suggested by the Examiner, destroys the intent and purpose of "Dillon 911 taken alone or in view of Dillon '467 is the use of "key seed Ids" used for decrypting keys. Accordingly, the present invention is distinguishable over Dillon 911 taken alone or in view of Dillon '467 for this reason as well.

Continuing further, when there is no suggestion or teaching in the prior art for a first encrypting key which is a symmetric key, the suggestion cannot come from the Applicants' own specification. The Federal Circuit has repeatedly warned against using the Applicants' disclosure as a blueprint to reconstruct the claimed invention out of isolated teachings of the prior art. See MPEP §2143 and Grain Processing Corp. v. American Maize-Products, 840 F.2d 902, 907, 5 USPQ2d 1788 1792 (Fed. Cir. 1988) and In re Fitch, 972 F.2d 160, 12 USPQ2d 1780, 1783-84 (Fed. Cir. 1992). The prior art reference Dillon '911 taken alone or in view of Dillon '401 does not suggest, teach, or mention the use of "symmetric" encrypting keys for securing content.⁴ Dillon does make use of symmetric keys for managing account statistics, billing and other non-content related encryption at col. 5, lines 23-37. However, Dillon explicitly teaches away from the use of symmetric keys for encrypting the content and instead describes a key seed ID.

For the foregoing reasons, independent claims 1, 7, 19, and 21 as amended distinguish over Dillon '911 in view of Dillon '467. Claims 2-3, 5, 8-16, and 22-24 depend from claims 1, 7, and 21 respectively, since dependent claims contain all the limitations of the independent claims, claims 2-3, 5, 8-16, and 22-24 distinguish over Dillon '911 taken alone or in view of Dillon '401, as well, and the Examiner's rejection should be withdrawn.

⁴ Very recently, the Federal Circuit again took up the identical question of Obviousness in combining references in the case In re Sang Su Lee, No. 00-1158 (January 18, 2002). In this case Board of Patent Appeals rejected all of Applicant's pending claims as obvious under § 103. The Federal Circuit vacated and remanded. Citing two prior art references, the Board stated that a person of ordinary skill in the art would have been motivated to combine the references based on "common knowledge" and "common sense," but it did not present any specific source or evidence in the art that would have otherwise suggested the combination. The Federal Circuit held that the Board's rejection of a need for any specific hint or suggestion in the art to combine the references was both legal error and arbitrary agency action subject to being set aside by the court under the Administrative Procedure Act (APA). Accordingly, with the suggestion or motivation found in Johnson, the Examiner has failed to properly establish a *prima facie* case of obviousness of the invention as a "whole." The Applicants submit the present invention distinguishes over Dillon 911 taken alone or in view of Dillon '467 for at least this reason as well.

Rejection Under 35 U.S.C. §103(a) applying CableVision(Periodical)

As noted above, the Examiner rejected claims 4 and 6 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467), and further in view of Cablevision(periodical). Independent claim 1 has been amended to distinguish over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467) as described above. The Examiner goes on to combine CableVision(periodical).⁵ The Cablevision reference nowhere suggests or teaches “symmetric key” and “encrypting the first decrypting key, using a second encrypting key.” Accordingly, claim 1 of the present invention distinguishes over Dillon ‘911 in view of Dillon ‘467, and further in view of Cablevision(periodical). Claims 4 and 6 depend from claim 1, since dependent claims contain all the limitations of the independent claims, claims 4 and 6 distinguish over Dillon ‘911 taken alone or in view of Dillon ‘401, and further in view of Cablevision(periodical) as well, and the Examiner’s rejection should be withdrawn.

Rejection Under 35 U.S.C. §103(a) applying Horstmann (US 6,009,401)

As noted above, the Examiner rejected claims 17 and 18 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467) as applied to claim 7 above, and further in view of Horstmann (U.S. 6,009,401). Independent claim 1 has been amended to distinguish over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467) as described above. The Examiner goes on to combine Horstmann.⁶ Horstmann nowhere suggests or teaches “symmetric key” or “encrypting the first decrypting key, using a second encrypting key”. Accordingly, claim 7 of the present invention distinguishes over Dillon ‘911 in view of Dillon ‘467, and further in view of Horstmann. Claims 17 and 18 depend from claim 7, since dependent claims contain all the limitations of the independent claims, claims 17 and 18 distinguish over Dillon ‘911 taken alone or in view of Dillon ‘401, and further in view of Horstmann as well, and the Examiner’s rejection should be withdrawn.

⁵ Applicants make no statement whether such combination is even proper.

⁶ Applicants make no statement whether such combination is even proper.

CONCLUSION

Applicants have examined the reference cited by the Examiner as pertinent but not relied upon. It is believed that this reference neither discloses nor makes obvious the invention recited in the present claims.


In view of the foregoing, Applicants respectfully submit that all of the grounds for rejection stated in the Examiner's office action have been overcome, and that all claims in the application are allowable. No new matter has been added. It is believed that the application is now in condition for allowance, which allowance is respectfully requested.

PLEASE CALL the undersigned if this would expedite the prosecution of this application.

Respectfully submitted.

January 27, 2003

By: _____


Jon A. Gibbons (Reg. No. 37,333)
Attorney for Applicants
Fleit, Kain, Gibbons, Gutman & Bongini, P.L.
One Boca Commerce Center, Suite 111
551 Northwest 77th Street
Boca Raton, FL 33487
Telephone: (561) 989-9811
Facsimile: (561) 989-9812

PLEASE Direct All Correspondence to Customer Number 23334



150-a99-164amd1-af.wpd

SE9-99-020

Page 17 of 17

09/487,417